THÉORIE DES GROUPES. — *Point générique du plus petit groupe algébrique dont l'algèbre de Lie contient plusieurs matrices données.* Note (*) de **Christophe Reutenauer**, présentée par Jacques Tits.

On étend au cas de plusieurs matrices la formule de Chevalley donnant un point générique du plus petit groupe algébrique dont l'algèbre de Lie contient une matrice donnée.

We extend to the case of several matrices Chevalley's formula giving a generic point of the smallest algebraic group whose Lie algebra contains a given matrix.

1. Soit k un corps commutatif de caractéristique nulle. C. Chevalley a montré que pour toute matrice $M \in k^{n \times n}$ (l'algèbre des $n \times n$ matrices à coefficients dans k), le plus petit groupe algébrique dont l'algèbre de Lie contient M admet comme point générique la matrice $\exp(a\,M)$, à coefficients dans le corps des séries formelles en l'indéterminée a [4] (th. 10, § 13). Le but de cette Note est de montrer qu'on obtient un résultat analogue dans le cas de plusieurs matrices, par l'utilisation des séries formelles en variables non commutatives, mais munies d'un produit commutatif : le mélange ou produit de Hurwitz (en anglais : shuffle product). Ce produit a été introduit par R. Ree [8] pour la caractérisation des éléments de Lie dans une algèbre libre et formalise une propriété remarquable des intégrales itérées de K. T. Chen [3]. En fait, le produit de Hurwitz des séries formelles correspond à la structure d'algèbre de Hopf de l'algèbre associative libre, considérée comme bigèbre enveloppante de l'algèbre de Lie libre ([1], [9]).

Faisons d'abord la remarque suivante. Sur $k[[a]]$, considérons le produit associatif défini par :

$$(a^i, a^j) \mapsto \binom{i+j}{i} a^{i+j},$$

que nous notons $a^i \sqcup\!\sqcup\, a^j$. On a alors $a^{\sqcup\!\sqcup\, n}$ (= la puissance n-ième de a pour ce produit) $= n!\, a^n$. Par conséquent l'exponentielle de la matrice $a\,M$ pour ce produit est la matrice :

$$\exp_{\sqcup\!\sqcup}(a\,M) = \sum_{n \geqq 0} a^n M^n,$$

qui est égale à l'inverse de $1 - a\,M$ considérée comme matrice à coefficients dans $k[[a]]$ muni du produit usuel.

Par commodité, nous appellerons *algèbre de Cauchy* l'algèbre $k[[a]]$ munie du produit usuel et *algèbre de Hurwitz* l'algèbre $k[[a]]$ munie du produit $\sqcup\!\sqcup$. De plus nous noterons $(a\,M)^*$ l'inverse de $1 - a\,M$ dans l'algèbre de Cauchy : $(a\,M)^* = (1 - a\,M)^{-1}$, appelée *l'étoile* de $a\,M$.

Ainsi le groupe algébrique considéré ci-dessus admet pour point générique l'étoile de $a\,M$, mais considérée comme élément de l'algèbre de Hurwitz. C'est sous cette forme que nous étendons la formule de Chevalley.

2. Soit A un ensemble fini que nous appellerons *alphabet*, et dont les éléments sont des *lettres*. A^* désigne le monoïde libre engendré par A. Ses éléments sont des mots et son élément neutre (le mot vide) est noté 1. Une *série formelle* est une application :

$$S : A^* \to k,$$

On la note $S = \sum_{w \in A^*} (S, w) w$ où (S, w) est l'image du mot w, ou son *coefficient*. Nous notons $k \langle\langle A \rangle\rangle$ l'ensemble des séries formelles et $k \langle A \rangle$ l'ensemble des polynômes (un polynôme est une série de support fini). On définit sur $k \langle\langle A \rangle\rangle$ deux structures d'algèbre sur k. D'une part, l'algèbre de Cauchy, dont le produit étend à $k \langle\langle A \rangle\rangle$ le produit sur A^*. On a donc pour deux séries formelles S et T :

$$(ST, w) = \sum_{uv = w} (S, u)(T, v).$$

L'algèbre de Cauchy n'est pas commutative si $|A| \geqq 2$.

D'autre part l'algèbre de Hurwitz : pour cela, si $w = a_1 \ldots a_n (a_i \in A)$ est un mot et I une partie de $\{1, \ldots, n\}$, $I = \{i_1 < i_2 < \ldots < i_k\}$, notons $w(I) = a_{i_1} \ldots a_{i_k}$. On définit alors le produit de Hurwitz de deux mots $u = a_1 \ldots a_p$, $w = b_1 \ldots b_q (a_i, b_j \in A)$ comme le polynôme :

$$u \sqcup\!\sqcup v = \sum w_{I, J},$$

où la somme est étendue à toutes les partitions $\{1, \ldots, p+q\} = I \cup J$ telles que $|I| = p$, $|J| = q$ et où le mot $w_{I, J}$, de longueur $p+q$ est défini par $w_{I, J}(I) = u$ et $w_{I, J}(J) = v$. On convient que $1 \sqcup\!\sqcup u = u \sqcup\!\sqcup 1 = u$.

Exemple. – $ba \sqcup\!\sqcup ab = 2\,baab + baba + abab + 2\,abba$. Il n'est pas difficile de voir que ce produit coïncide avec celui que nous avons défini au paragraphe 1 dans le cas d'une seule lettre. On l'étend par linéarité et continuité aux séries formelles (avec la topologie usuelle sur $k \langle\langle A \rangle\rangle$) : le produit de Hurwitz est commutatif et associatif. De plus il est intègre ([8], th. 3.2). L'algèbre de Hurwitz possède donc un corps de fractions que nous notons K.

Nous aurons à considérer l'algèbre $k \langle\langle A \rangle\rangle^{n \times n}$ des matrices d'ordre n à coefficients dans $k \langle\langle A \rangle\rangle$, tantôt avec le produit de Cauchy, tantôt avec le produit de Hurwitz. Si M est une telle matrice, elle est dite *propre* si les séries formelles coefficients de M ont toutes un terme constant nul; on définit alors *l'étoile* de M par la formule (dans l'algèbre de Cauchy) :

$$M^* = (1 - M)^{-1} = \sum_{n \geqq 0} M^n.$$

Venons-en au théorème. Soient $\mathcal{M}$ un ensemble fini de matrices dans $k^{n \times n}$ et A un alphabet en bijection avec $\mathcal{M}$: la bijection est notée $\mu : A \to \mathcal{M}$ et elle s'étend en un homomorphisme multiplicatif $\mu : A^* \to k^{n \times n}$. Nous posons :

$$M = \sum_{a \in A} a . \mu a \in k \langle\langle A \rangle\rangle^{n \times n}.$$

THÉORÈME. – *La matrice* M^* (*considérée dans l'algèbre de Hurwitz, donc dans* K) *est un point générique du plus petit groupe algébrique dont l'algèbre de Lie contient* $\mathcal{M}$.

3. *Démonstration du théorème.* – Soit G le plus petit groupe algébrique dont l'algèbre de Lie $\mathcal{L}$ contient $\mathcal{M}$. Nous montrons d'abord que M^* est un point généralisé de G, en utilisant une généralisation de la formule de Baker-Campbell-Hausdorff, dûe à R. Ree ([8], th. 2.5), il y démontre que si L est une $\mathbb{Q}$-algèbre commutative et :

$$S = \sum_{w \in A^*} (S, w) w \in L \langle\langle A \rangle\rangle \quad \text{(algèbre de Cauchy)},$$

de terme constant $(S, 1) = 1$, alors $\log S$ est un élément de Lie si et seulement si la forme L-linéaire sur $L \langle\langle A \rangle\rangle$ définie par $w \mapsto (S, w)$ est un homomorphisme de l'algèbre de Hurwitz $L \langle\langle A \rangle\rangle$ dans L.

En particulier, si $L = k\langle\langle A\rangle\rangle$ (structure de Hurwitz) et $(S, w) = w$, la série $\log S$ est un élément de Lie. Soit $(P_i)_{i\in I}$ une base de la $\mathbb{Q}$-algèbre de Lie engendrée par A dans $L\langle\langle A\rangle\rangle$ (structure de Cauchy). On a donc :

$$\log S = \sum_{i\in I} H_i P_i,$$

avec $H_i \in L$. Par suite :

$$\log S = \sum_{i\in I}\Big(\sum_{w\in A^*}(H_i, w)\,w\Big)P_i = \sum_{w\in A^*} w\Big(\sum_{i\in I}(H_i, w)P_i\Big) = \sum_{w\in A^*} w\,Q_w,$$

où :

$$Q_w = \sum_i (H_i, w)\,P_i,$$

est un élément de Lie de $k\langle\langle A\rangle\rangle$.

Or la relation :

$$\log S = \sum_{n\geq 1}\frac{(-1)^{n+1}}{n}\Big(\sum_{w\in A^*\setminus 1}(S, w)\,w\Big)^n,$$

montre que Q_w est un polynôme homogène de degré $|w|$ (=longueur du mot w).

Par ailleurs :

$$M^* = \Big(\sum_{a\in A} a.\mu a\Big)^* = \sum_{n\geq 0}\Big(\sum_{a\in A} a.\mu a\Big)^n = \sum_{w\in A^*} w.\mu w.$$

Considérant M^* comme l'élément de $k\langle\langle A\rangle\rangle^{n\times n}$ muni du produit de Hurwitz et appliquant ce qui précède, on a donc :

$$\log M^* = \sum_{w\in A^*\setminus 1} w.\mu(Q_w),$$

où l'on a prolongé μ en un homomorphisme d'algèbres $k\langle A\rangle \to k^{n\times n}$ (structure de Cauchy) et où $\mu(Q_w)$ appartient donc à l'algèbre de Lie engendrée par $\mathscr{M}$, donc à $\mathscr{L}$. Par conséquent, chaque $w.\mu(Q_w)$ est un point généralisé (à coefficient dans K) de $\mathscr{L}$, donc $\log M^*$ est un point généralisé de $\mathscr{L}$. Par suite M^* est un point généralisé de G. Soit $a\in A$ et considérons l'homomorphisme $k\langle\langle A\rangle\rangle \to k[[a]]$ (structures de Hurwitz) qui envoie a^i sur lui-même et tout mot contenant une lettre autre que a sur 0. L'image de M^* est la matrice $(\sum a.\mu a)^* = \exp_{ш}(a.\mu a)$, comme remarqué au paragraphe 1. Ce point est donc spécialisation de M^*. Pour conclure il suffit donc de montrer que les points dans $GL_n(k)$ qui sont spécialisations de M^* forment un sous-groupe de G. Cela se ramène à montrer que le produit de deux spécialisations de M en est encore une [4] (prop. 2, § 1). Pour cela, considérons l'application linéaire $\theta : k\langle\langle A\rangle\rangle \to k\langle\langle A\rangle\rangle \otimes k\langle\langle A\rangle\rangle$ définie par $\theta(w) = \sum_{uv=w} u\otimes v$. On vérifie aisément que θ est un homomorphisme d'algèbres de Hurwitz (*voir* aussi [3], th. 1.8). L'image de M^* par θ est :

$$\sum_{w\in A^*}\theta(w).\mu w = \sum_w\Big(\sum_{uv=w} u\otimes v\Big).\mu w = \sum_{u,v} u\otimes v.\mu u.\mu v = \Big(\sum_u (u\otimes 1).\mu u\Big)\Big(\sum_v (1\otimes v).\mu v\Big),$$

considéré comme élément de $(k\langle\langle A\rangle\rangle \otimes k\langle\langle A\rangle\rangle)^{n\times n}$.

Soient alors E et F dans $GL_n(k)$ des spécialisations de M^*. Il existe alors deux homomorphismes φ et ψ de la sous-algèbre de Hurwitz $\mathscr{A}$ de $k\langle\langle A\rangle\rangle$ engendrée par les coefficients de M^* dans k tels que $\varphi(M^*)=E$ et $\psi(M^*)=F$. L'élément (i, j) de la matrice $\theta(M^*)$ est égal à $\sum_k [(M^*)_{ik}\otimes 1][1\otimes(M^*)_{kj}]$ donc appartient à $\mathscr{A}\otimes\mathscr{A}$. D'où un homomorphisme $(\varphi\otimes\psi)\circ\theta : \mathscr{A}\rightarrow k$ qui applique M^* sur EF.

4. Signalons que le théorème ci-dessus s'applique en théorie de la controlabilité des systèmes réguliers en automatique non linéaire, *via* le théorème de Kleene-Schützenberger ([5], il caractérise la *rationalité* des séries formelles non commutatives à l'aide de matrices M^* comme ci-dessus), la théorie de Fliess [7] et l'algèbre différentielles. Mais ceci sera exposé par ailleurs.

(*) Remise le 12 octobre 1981.

[1] N. BOURBAKI, *Groupes et algèbres de Lie*, chap. II, § 1, Hermann, Paris.

[2] K. T. CHEN, *Ann. of Math.*, 65, 1957, p. 163-178.

[3] K. T. CHEN, *J. Algèbre*, 9, 1968, p. 1-36.

[4] C. CHEVALLEY, *Théorie des groupes de Lie*, II, Groupes algébriques, Hermann, Paris.

[5] S. EILENBERG, *Automata, Languages and Machines*, A, Acad. Press, New York, 1974.

[6] M. FLIESS, *J. Math. Pures Appl.*, 53, 1974, p. 197-222.

[7] M. FLIESS, in *Math. Systems Theory*, 6, MARCHESINI et S. K. MITTER, éd., *Lect. Notes Econom. Math. Syst.*, 131, Springer-Verlac, Berlin, 1976, p. 122-148.

[8] R. REE, *Ann. of Math.*, 68, 1958, p. 210-220.

[9] M. E. SWEEDLER, *Hopf algebras*, W. A. Benjamin, New York, 1969.

Institut de Programmation,
4, *place Jussieu*, 75230 *Paris Cedex* 05.